International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 3 244 – 247

Mobile Cloud Encrypted Searching and Traffic Reduction

Pavan Kulkarni, Aditya More, Ganesh Pawar, , Sushil Padghan, Rahul Patil
Pavan Kulkarni, Assistant Professor, Computer Dept, TCOER, Pune
Aditya More, Computer Dept, TCOER, Pune
Ganesh Pawar, Computer Dept, TCOER, Pune
Sushil Padghan, Computer Dept, TCOER, Pune
Patil Rahul, Computer Dept, TCOER, Pune

ABSTRACT: Now days, cloud infrastructure have been popular for storing data in the world. User can store his public and private data on cloud. To secure the private data it must be encrypted. This encrypted data should be retrieved and stored efficiently. This era is digital era. Nearly about each person has mobile phone. So smart phone would be the best client for the cloud. But using smart phone use wireless network which face many difficulties like low bandwidth, low latency, low battery, low transmission etc. The traditional search is not developed on focusing on smart phone so using smart phone it require the extra network traffic and long time for search. The application use the light weight trapdoor which reduce trapdoor size and provide feasible method for the network traffic efficiency. Also it use and Ranked Serial Binary Search algorithm 0and Trapdoor Mapping Table (TMT) to minimize the search time. The proposed system reduce the search time and network traffic**.**

Keywords: *Mapping Table, Compression, Ranking Search, Encrypted Search, Mobile Cloud.*

*****

I. INTRODUCTION

This is an android app and web app through which we can share and manage centralized library. Web apps contains Admin section which uploads and manages college's academic books related data. Web app also contains office section where EBC and scholarship forms are filled up by students through Android application will be shown on Web Application with the documents attached by students. In Android application only registered students can get logged in through their respective unique PRN numbers. Student can download, search, uploaded books by admin after successful login. Students are having privileged to upload books by their own. Android application contains the facilities to fill up the EBC and scholarship forms. The application uses the light weight trapdoor which reduce trapdoor size and provide feasible method for the network traffic efficiency. Also it uses Ranked Serial Binary Search algorithm and Trapdoor Mapping Table (TMT) to minimize the search time. The proposed system reduces the search time and network traffic.

According to our calculation and analysis, a search call in the previous system could form trapdoors with a space up to1.2MB.When displaying search calls, the trapdoor has to be transfer two times (step 7 and 8). In such scenario, privacy-protective searches could hint to lengthy search delay and larger bandwidth absorption, which could not be cheap to mobile handlers or users. This analysis targeted on traffic and search time inefficiency problems over the mobile cloud. We present an efficient Encrypted Data Search and Traffic Reduction as Mobile cloud services scheme to overcome these issues. Our application is focuses on multi-keyword privacy-protection search and highly step down network traffic and search delays. For network traffic, our proposed system pre-calculate trapdoors for similar search keywords and thus stops one network. Round hops for re-calculating trapdoor per calls. We additionally designs several elements to compact trapdoors and provide demo that our pre-calculated trapdoor table has a space of 0.31MB and could be efficiently record and loaded in mobile device storage. In reference of search time, our system application calculate the search algorithm in the cloud. On the basis of the binary tree principle, we provide Ranked Serial Binary Search (RSBS) algorithm, which could loses query time in the cloud. Our dedication can be examined as follows:

1) We check out the previous encrypted search architecture in reference of network traffic and search time. Results point out that the efficient approach is not applicable in mobile-cloud infrastructure.
2) We designed our system application to point out these challenges. Our architecture consists a trapdoor reduction technique to compress traffic costs, as well as a Trapdoor Mapping Table (TMT) model and RSBS algorithm to compress search time.
3) We examine the efficiency of our system in network traffic and search time. We denote that with our system architecture, we can deduct network traffic.

II. ALGORITHMS

2.1 FAH ALGORITHM: FAST ACCUMULATED HASHING

A new no trapdoor accumulator for cumulative hashing is introduced. It can be efficiently realized in practice using existing cryptographic hash algorithms and pseudorandom sequence generators. The memory requirement is less than in comparable signature based solutions.

Algorithm 1 Trapdoor Generation Process

Input:
Keyword: K
Hash function in FAH algorithm: $H()$
Mapping function in FAH algorithm: $G()$
Noise set: $\Theta = \{\varepsilon_1, \varepsilon_2, \ldots \varepsilon_p\}$
Output:
Index: Compressed trapdoor $\bar{\tau}_t{}'$
1: Extract the term t from K.
2: **if** the term t hits in the TMT module **then**
3: Obtain its pure trapdoor without any noise.
4: **else**
5: Hash it by $H()$ and get its l-bit hash code $\tau_t = H(t)$; Map τ_t to $\bar{\tau}_t = \{0,1\}^r$ by $G()$, which contains r bits
6: **end if**
7: Choose q noises from the noise set Θ to build a subset $\varepsilon = \{\varepsilon_1, \varepsilon_2, \ldots \varepsilon_q\}$, and accumulate it with $\bar{\tau}_t$ to get $\bar{\tau}_t \bigwedge \varepsilon$.
8: Calculate the location of each characteristic bit 0 in $\bar{\tau}_t \bigwedge \varepsilon$ by utilizing an m-bit $\{0,1\}$ codes to record this location ($r = 2^m$), accumulate values of locations in order $\underbrace{\{0,1\}^m \bigwedge \{0,1\}^m \bigwedge \ldots \{0,1\}^m}_{f}$, get a compressed trap-

2.2 RSS ALGORITHM: RANKED SERIAL SEARCH. Cryptographic: (a process called encryption)

Cryptography is a method of storing and transmitting data in particular form so that only those for whom it is intended can read and process it.

Plaintext:
Most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext).

Cliphertext:
Ciphertext is then back again (known as decryption). Individuals who practice this field are known as cryptographers.

2.3 RSBS ALGORITHM: RANKED SERIAL BINARY SEARCH

LSB: Last significant bit
CBS: Centre Bit Signification

Algorithm 2 Ranked Serial Binary Search (RSBS) algorithm

Input:
Noised trapdoors (one per search keyword): $\bar{\tau}_1{}', \ldots, \bar{\tau}_\varepsilon{}'$
Encrypted document indexes: $A = \bar{I}_1{}' \cdots \bar{I}_N{}'$
The number of documents to return: k
Output:
Top-k documents that best match the search request: $D = \{D_1, D_2, \cdots, D_k\}$
1: $Scores = zeros\{0, N\)$ // create an array of N zeros
2: **for** $i := 1$ **to** N **do**
3: **for** $n := 1$ **to** ε **do**
4: Score[i] ← Score[i] + bsearch($\bar{\tau}_n{}', \bar{I}_i{}', 1, s_i$) // search if the keyword appears in any of the s slices of the document
5: **end for**
6: **end for**
7: sorted, indices = sort($Scores$) // sort the score array and get the indices or old element in the sorted array.
8: $D \leftarrow indices[0 : k-1]$ // get the top-k documents
9: **return** D

III. SYSTSEM OVERVIEW

In this we will discuss and analyze about the developing architecture of Efficient Encrypted search and traffic reduction as mobile cloud services. This will help user to manage the ebooks and other document in electronic format. It also reduces the risk of paper work such as encryption of such important documents. It gives the proper reliability. This architecture also provide the proper utilization of network traffic as well as searching time.

System architecture consist of
-User Module
-Admin Module

student PRN no. Which is stored in SQLite database.

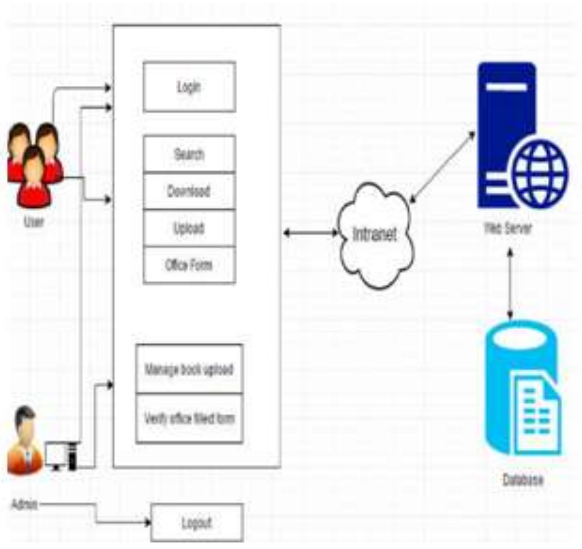

Figure 1: System Architecture

User Module-
The user module is basically designed for the student who need to login first as per above diagram. Student first login with his given PRN no. After login successfully they allow

to upload his data, books or other stuffs on the cloud with the help of it's mobile device. Student or system also provide search and download term within cloud. This system mostly focus on the eliminating the number of trips by using some mapping table that will help to improve in search and download.

Admin Module-

This architecture also contain the admin module which contain separate login when admin logon to system. Admin verifies the uploaded document. They are also able to access all the document over cloud. They keep and verifies the document and whenever required it generates encryption key.

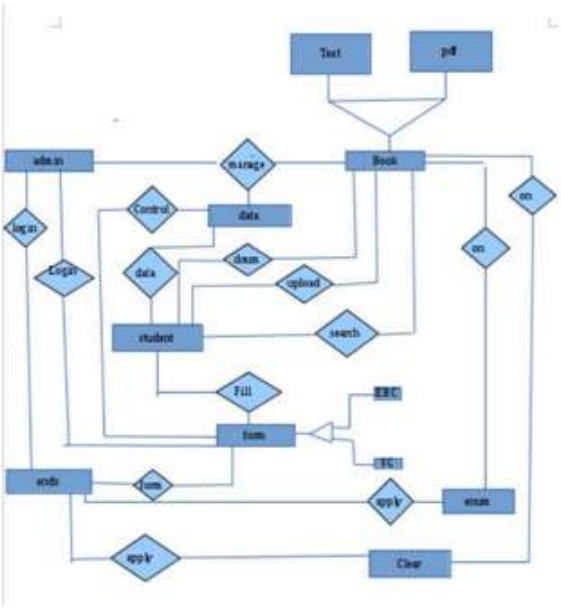

Figure 2: Activity diagram of system

4.1 Searching-

This screen uses in book maintenance part. We search a book based on book_id, book name, publication or by author name. System will search the keyword in the cloud. System is able to filter a book based on keyword entered. It scans as per the mapping index and it shows the result faster manner as compare to previous system.

After this system provides the download option which download the document as fast as possible. System is also provide the personal downloads then there is upload option for upload of different document. This will see publically on cloud.

The system also provide encryption for important document for better reliability. The admin whenever logon to the system they are allow or authorities to handle different forms and document (for verification)

IV. IMPLEMENTATION

In this system we need to analyze some of objective for better implementation of system. Some of the objective are like improvement in control and performance the system is developed to cap up with the current issue and problems. The system can add user, validate user and is also bug free. Save time is also important user and admin is able to search record by using few click of buttons and few search keywords thus saving the valuable time. System should provide facility to upload files or note in a pdf file having size not more than 15 Mb.

In implementation we forms some of the screens are firstly user login. This feature used by the user to login into system. They are required User_ id and password before they allow to enter the system. User_Id is allocate by

V. ACKNOWLEDGEMENT

This work was supported by Computer Dept. of Trinity college of Engineering and Research, Pune. Under guidance of prof. Pavan Kulkarni, Pornima Gaikwad and students and all respected staff members. Thankful for those who are directly and indirectly involved in this project.

VI. CONCLUSION

1) We figure out the previous encrypted search system and understand their limitations while using the mobile cloud. This system was required more network and search time.
2) Thus we developed the "Efficient Encrypted Searching and Traffic Reduction. As Mobile cloud Service" which and reduce the limitations addressed by the mobile cloud.
3) We use Ranked Serial Binary Search algorithm and Trapdoor Mapping Table (TMT) to minimize the search time. The proposed system reduces the search time and network traffic

REFERENCE

[1] D. Huang, “Mobile Cloud Computing,” Ieee Comsoc Multimedia Commun. Tech. Committee (Mmtc) E-Letter, Vol. 6, No. 10, Pp. 27– 31, 2011.

[2] N. Cao, C. Wang, M. Li, K. Ren, And W. Lou, “Privacypreserving Multi-Keyword Ranked Search Over Encrypted Cloud Data,” In Proc. Int. Conf. Comput. Commun. (Infocom), Apr. 2011, Pp. 829–837

[3] C. Wang, N. Cao, K. Ren, And W. Lou, “Enabling Secure And Efficient Ranked Keyword Search Over Outsourced Cloud Data,” Ieee Trans. Parallel Distrib. Systems, Vol. 23, No. 8, Pp. 1467–1479, 2012.

[4] C. Wang, N. Cao, J. Li, K. Ren, And W. Lou, “Secure Ranked Keyword Search Over Encrypted Cloud Data,” In Proc. Ieee Int. Conf. Distrib. Comput. Syst. (Icdcs), Jun. 2010, Pp. 253–262.

[5] C. Gentry And S. Halevi, "Implementing Gentrys Fullyhomomorphic Encryption Scheme," In Advances In Cryptology– Eurocrypt 2011, 2011, Pp. 129–148.

[6] C. Orencik And E. Savas¸, "Efficient And Secure Ranked Multi- ¨ Keyword Search On Encrypted Cloud Data," In Proc. Joint Edbt/Icdt Workshops, Mar. 2012, Pp. 186–195.

[7] Gartner, "Worldwide Traditional Pc, Tablet, Ultramobile And Mobile Phone Shipments On Pace To Grow 7.6 Percent In 2014," Http://Www.Gartner.Com/Newsroom/Id/2645115.

[8] Trellian, "Keywords Number," Http://Www.Keyworddiscovery. Com/Keywordstats.Html?Date=2014-03-01.

[9] V. Rijmen And J. Daemen, "Advanced Encryption Standard," Federal Information Processing Standard, Pp. 19–22, 2001.

[10] X. Lai, "On The Design And Security Of Block Ciphers," Ph.D. Dissertation, Diss. Techn. Wiss Eth Zurich, Nr. 9752, 1992. Ref.: ¨ Jl Massey; Korref.: H. Buhlmann.